FIFTH ARMY INPROCESSING INFORMATION

ARRIVAL DATE: _____ **DUTY TEL:** _____

UNIT: _____ **(If recruiter, which battalion?)** _____

NAME: _____

SSN: _____ **RANK:** _____

DATE OF BIRTH: _____ **PLACE OF BIRTH:** _____
(State)

If <u>not</u> born in the U.S., check one:
Born to U.S. citizens abroad _____ *Naturalized Citizen* _____

OTHER NAMES USED: _____
(Aliases, maiden, former marriages)

ANY BREAKS IN SERVICE (Dates): _____

Civilian Only
SERVICE COMPUTATION DATE: _____

Military Only *Circle One*
PRIMARY MOS: _____ **STATUS: RA USAR AGR Other** _____

BASIC ACTIVE SERVICE DATE (BASD): _____

PAY ENTRY DATE BASIC DATE (PEBD): _____

The following items also require an answer:

a. Do you have a copy of your SF 312 from your last duty station? YES NO

b. Were you indoctrinated in the SCI Program at your last duty station: YES NO

c. Were you debriefed prior to departing your last duty station? YES NO

d. Are you pending/awaiting a periodic reinvestigation update? YES NO

SIGNATURE _____
DATE _____

NOTICE: In compliance with The Privacy Act, 5 U.S.C. 552a, the disclosure of the social security number is voluntary. However, Executive Order 9397 authorized DA to use the SSN as a system to identify Army members and employees, but disclosure is voluntary. Your failure to do so may impede the processing of such certifications and determinations for access to security information.

SECURITY ORIENTATION BRIEFING

1. Topics covered in this security orientation briefing were taken directly from FORSCOM Suppl 1 to AR 380-5. Every topic listed is required for both initial and refresher security training.

a. Principals of the Security Program. The security program is necessary for America's survival. The policy established in AR 380-5 on the classification, downgrading, declassification, transmission, transportation and safeguarding information is vital to the interests of our national security. Protecting classified and other information that requires protection is an individual, non-waiverable responsibility.

b. Classification Levels. Collateral classified information falls into 3 different categories.

(1) CONFIDENTIAL: Information that, if compromised, could cause some damage to our national security.

(2) SECRET: Information that, if compromised, could cause serious damage to our national security.

(3) TOP SECRET: Information that, if compromised, could cause exceptionally grave damage to our national security.

c. Security Clearance Requirements: You will be required, when applicable by either your MOS or duty position, to have a security clearance. Both the requisite clearance and access level is required before you can accept any classified information. You have a personal responsibility NOT to accept classified information to which you have no authority to accept. Your Security Manager will advise you of your appropriate clearance requirements.

d. SF 312 – Classified Information Non-disclosure Agreement. (A legally bonding agreement.) The purpose of the SF 312 is to warn you of the consequences of illegally passing classified information to which you are entrusted, to anyone who does not have the authority to accept it and it is effective for the rest of your life! It also warns you of the consequences of passing classified information to foreign governments (Espionage). There is an original copy of the form in your field military 201 file which has a disposition of 75 years after you leave the military service. Your signature on this form signifies that under those consequences, you accept the responsibility to protect our national security. Signing the SF 312 is a mandatory prerequisite to having a clearance and access. You are hereby advised that any breach of this agreement may result in the termination of your security clearance, removal from my position, termination of employment, and that you can be prosecuted for violations of United States Code criminal laws.

e. Need-to-Know: Having a security clearance and access to classified information does not mean you have access to all classified information relative to the level of your clearance. Every individual has a personal, non-waiverable responsibility to ensure that any classified information that you either accept from another person, or that you give to another person is necessary for you or that person.....PERIOD. This is particularly true for contractors, who are limited only to that information stated in their contract. You MUST establish need-to-know before sharing classified information.

f. Legal Statutes: The DA Information Security Program Regulation uses Presidential Executive Order 12958 as it's legal authority. Titles 5, 10 and 18 of the United States Code also address restrictions and punishments for the illegal use of classified information. If you would like to see these statutes, please ask your Security Manager.

g. Reporting Derogatory Information. If you are in possession of any creditable derogatory information about any US Army or Civilian member, you have a personal, non-waiverable, responsibility to report it to your Security Manager. The information should be kept close hold and should not be discussed with anyone except your Security Manager. Creditable derogatory information is a valuable tool in weeding out those personnel who are a risk to our national security. DON'T TAKE THAT CHANCE, REPORT IT!

h. Classification Principles: Information belonging to the US Army that must be protected from unauthorized disclosure is the principle of designating it with a security classification, restricted distribution, restricted reproduction, special access, or other caveated designations that control that information. You must never violate the restrictions imposed by any of these markings.

i. Original Classification: At Fifth U.S. Army, the Commanding General has original classification authority up to the TOP SECRET level. This means that he/she has the authority to classify information up to the TOP SECRET level without using a derivative means to do so. If you have information that you believe that should be classified, but you have no derivative authority with which to classify it, please contact the Command Security Manager at 221-1909 for assistance.

j. Derivative Classification: Derivative classification is the act, by an appropriately cleared person with the authority to do so, to respond to, reshape, extract, or otherwise use a derivative classifier as an authority to produce a new classified document. A derivative classifier expressed on the classification authority (DERIVED FROM) line, can be a security classification guide, a message, a printed directive, a memorandum, an OPLAN, or other document.

k. Duration of Classification: An original classifier (i.e. the HQ5A Commanding General) must select a date not more than 10 years out, an event certain to occur, or a 25-year exemption when authorized in which that information will become declassified or mandates a review for declassification – on all original classification decisions. Many security classification guides, printed directives and messages prescribe a declassification date. In even a declassification date is not prescribed, you must then carry forward the most restrictive declassification instruction from the derivative document used to classify your document.

l. Security Classification Guide: A security classification guide contains written instructions on what information is to be classified and for how long for a specific classified end item, weapon, exercise, OPLAN, etc. The guide is required to be printed before the item is produced.

m. Classification Challenges: Every individual has a personal responsibility to challenge the classification of any information they feel is either over classified, under classified, or not classified at all. Contact the Command Security Manager at 221-1909 for assistance with your challenge.

n. Classification Markings: Classification Markings are required for the protection, storage and accountability of all classified documents. Derivatively classified documents must show the following:

(1) Identification of the office of origin.

(2) Classification following the subject (i.e. (U) (S) (TS) etc.

(3) The classification authority on the face of the document expressed as DERIVED FROM and citing the document or documents used to classify your document.

(4) Declassification/downgrading instructions expressed as DECLASSIFY ON and using the most restrictive declassification instructions from your source documents(s).

(5) Page markings, top and bottom of title page, first page, and last page. Interior pages will be marked with the highest level of classified information contained on that page.

(6) Portion Markings: Mark all paragraphs, portions, bullets, etc with the highest level of information contained in that portion (i.e. "(S). The elevation of Mount Download is SECRET".)

o. Declassification Principles/Exceptions: Declassification markings provide an appropriate declassification date for information that no longer needs to be classified in the interest of our national security. If you have any questions about documents that are exempted from automatic declassification, contact the Command Security Manager at 221-1909.

p. Reporting Suspicious Activities. You have a personal, non-waiverable responsibility to report security violations and creditable derogatory to your security manager; to report any high dollar equipment suspicious activities to the PMO Physical Security Office, any suspicious criminal activity to the PMO or CID Offices, and any suspicious activities regarding subversion or espionage to the Fort Hood Resident Officer, 902d MI Detachment, DSN 737-2507 or COMM (254) 287-2507.

q. Security Manager Program: Your Security Manager has been appointed by your local commander or staff division chief to represent them in all security matters. Please be advised that your Security Manager is your direct security link to your unit commander or staff division chief.

r. Accountability and Control Procedures: Classified information must be under the personal care and observation of a properly cleared individual, guarded by cleared personnel or stored in a GSA approved security container. It may also be openly stored in those areas which have been accredited in writing by the Command Security Manager.

s. Continuous Control and accountability:

(1) TOP SECRET and other specially marked information require a continuous chain of receipts.

(2) SECRET and CONFIDENTIAL information require a receipt only when mailed off the installation; however, you are required to keep a log or dispatch record of any SECRET or CONFIDENTIAL information that permanently leaves your jurisdiction.

t. Packaging/Transmission: SECRET and CONFIDENTIAL information may be sent via Registered, Certified (CONFIDENTIAL), FEDEX or US Postal Services Express mail. Bring classified to be mailed to your Security Manager or take it to the HQ5A Official Mail Room, Annex Building 44 before 0800 and 1300 every day. Classified information forwarded through the mail systems must first be wrapped in an inner envelope with the return address and addressee information, stamped or marked top and bottom front and back with the classification of the material inside, and all seams sealed with paper tape. The inner envelope is then placed in a plain outer envelope with only the return address and the addressee on it with all seams sealed with paper tape.

u. Physical Security Standards: Contact the PMO Physical Security Branch, 221-2222 if you need further information on physical security standards, motor pools, security of classified equipment, storage of high dollar and arms, ammunition and explosives.

v. Open Storage. See sub-paragraph r above.

w. Foreign Travel Briefings: Check with your security manager for required foreign travel briefings and clearances which are required prior to travel. If necessary, your security manager will coordinate with the Garrison Force Protection/Anti-Terrorism Program Manager to ensure your needs are met.

x. Foreign Personnel: Before you release any classified information to any foreign personnel, you should check with the Command Security Manager who also serves as the Foreign Disclosure Officer at 221-1909. There are strict procedures regarding this type disclosure with serious consequences for unauthorized disclosures to foreign personnel.

y. Contractors: If your mission or duties involve contractors, you should contact your security manager for any authorized classified disclosure to them. Access for contractors is as stated in their DD Form 254, contract agreement forms. When necessary, your Security Manager will contact the Command Security Manager also serving as the Industrial Security Manager at 221-1909 for assistance.

z. NATO information. See your security manager for a NATO read on if you are involved in access to NATO information. If your security manager is not authorized to provide you with a NATO brief and briefing statement, your security manager will ask the Command Security Manager for assistance in getting you read on. Access to information owned marked Stabilization Forces (SFOR) requires a NATO brief and read on.

2. KEY POINTS TO REMEMBER:

a. Telephones are not secure. Do not discuss classified or sensitive information over unsecure telephones.

b. Fax machines are also not secure. The HQ5A EOC has secure fax machines.

c. Protect your computer password at all times and do not share it with anyone.

d. Ensure you have proper authorization to hand carry and travel with classified material before you travel.

e. Keep classified documents separate from unclassified papers to prevent possible loss or compromise.

f. This unit and its mission is/may be a target of hostile intelligence or anti-government activities. Any attempts by anyone or agency to obtain classified or sensitive information must be reported immediately. If you feel that you have been approached by a person or agency attempting to gather classified or sensitive information, report the incident directly to this office or your security manager. DO NOT discuss the incident with anyone else.

g. Please out process through Ms. Margaret Plank, HQ5A Command Security Manager, Bldg. 16, Room 126, return all classified material to its control point and receive a security debriefing.

* ** * *

CERTIFICATE

I acknowledge that I have been granted access to classified and sensitive material, have been briefed on the working knowledge of the security requirements for handling this information, and the penalties for intentional or unintentional disclosure to unauthorized individuals or agencies.

SIGNATURE _____

PRINTED NAME _____

DATE _____